

UTILITY PATENT APPLICATION TRANSMITTAL (Only for new nonprovisional applications under 37 CFR 1.53(b))	Attorney Docket No. 1614.1010
	First Named Inventor or Application Identifier: Tsuneo SATO et al.
	Express Mail Label No.

APPLICATION ELEMENTS See MPEP chapter 600 concerning utility patent application contents.	ADDRESS TO: Assistant Commissioner Box Patent Application Washington, DC 20231
---	---

1. ☒ Fee Transmittal Form
2. ☒ Specification, Claims & Abstract [Total Pages: 39]
3. ☒ Drawing(s) (35 USC 113) [Total Sheets: 22]
4. ☒ Oath or Declaration [Total Pages: 3]
 - a. ☒ Newly executed (original or copy)
 - b. ☐ Copy from a prior application (37 CFR 1.63(d)) (for continuation/divisional with Box 17 completed)
 - i. ☐ **DELETION OF INVENTOR(S)**
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation by Reference (usable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein.
6. ☐ Microfiche Computer Program (Appendix)
7. ☐ Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary)
 - a. ☐ Computer Readable Copy
 - b. ☐ Paper Copy (identical to computer copy)
 - c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. ☒ Assignment Papers (cover sheet & document(s))
9. ☐ 37 CFR 3.73(b) Statement (when there is an assignee) ☐ Power of Attorney
10. ☐ English Translation Document (if applicable)
11. ☒ Information Disclosure Statement (IDS)/PTO-1449 ☒ Copies of IDS Citations
12. ☐ Preliminary Amendment
13. ☒ Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
14. ☐ Small Entity Statement(s) ☐ Statement filed in prior application, status still proper and desired.
15. ☒ Certified Copy of Priority Document(s) (if foreign priority is claimed)
16. ☐ Other:

17. If a CONTINUING APPLICATION, check appropriate box and supply the requisite information:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No:

18. CORRESPONDENCE ADDRESS

STAAS & HALSEY LLP
Attn: H. J. Staas
700 Eleventh Street, N.W., Suite 500
Washington, DC 20001

Telephone: (202) 434-1500
Facsimile: (202) 434-1501

09441034 11399
SPECIFICATION

TO ALL WHOM IT MAY CONCERN:

BE IT KNOWN THAT WE, Tsuneo Sato, a citizen of Japan residing at Kawasaki-shi, Kanagawa, Japan and Kiyoshi Kotegawa, a citizen of Japan residing at Oita-shi, Oita, Japan have invented certain new and useful improvements in

DEVICE AND METHOD FOR USER IDENTIFICATION
CHECK BASED ON USER-SPECIFIC FORMULA

of which the following is a specification : -

1 TITLE OF THE INVENTION

 DEVICE AND METHOD FOR USER IDENTIFICATION
CHECK BASED ON USER-SPECIFIC FORMULA

5 BACKGROUND OF THE INVENTION

 1. Field of the Invention

 The present invention generally relates to
 devices and methods for checking identification of
 users, an IC card for checking identification of the
10 owner of the card, and a memory medium having program
 recorded therein for checking identification of a user.
 The present invention particularly relates to a user-
 identification check method, a user-identification
 check device, and a user identification check card,
15 which achieve high security without imposing undue
 burden on users or on a system. The present invention
 further relates to a memory medium having a program
 embodied therein for achieving such a user-
 identification check device.

20 2. Description of the Related Art

 As a result of increasing use of computers in
 fabric of society, checking user identification based
 on a computer system has begun to be widely used in
 various fields relating to information processing. In
25 the event that checking of user identification errs or
 misuse of user identification is not prevented,
 ramifications are not only damages on individuals but
 also widespread confusion in society. Society demands
 a technology that achieves higher security in checking
30 of user identification.

 The scheme most widely used for user-
 identification check is to let a user to pick and
 register a pin code such as defined by 4 digits. When
 a user identification needs to be checked, the user
35 enters his/her pin code, and a check is made as to
 whether the entered pin code and the registered pin
 code match. A match indicates that the user is

1 authorized.

When a pin code is fixed as defined by a series of fixed digits, however, someone who sees a user entering a pin code may be able to pick up the code. This compromises security.

Further, users tend to select a pin code that is easy to remember for them, such as a selected portion of their phone number, the date of birth, the home address, etc. Such a tendency increases a chance of someone correctly guessing your pin number. This is also a factor to compromise security.

In order to obviate the drawbacks described above, Japanese Patent Laid-open Application No. 63-170764 teaches a system in which a user registers a formula and a key number. At a time of user-identification check, the system generates a time-dependent variable. A user enters a number that produces the key number when the entered number is inserted into the registered formula. The number entered by the user is compared with a number calculated by the system. If these two numbers match, the user is authorized.

In the user-identification-check system described above, a user registers a formula " $x + y$ " and a key number " $z_0 = 7$ ", for example. When the system presents a time-dependent variable 3 ($= x$), a user enters 4 ($= y$) that satisfies the equation " $x + y = 7$ ". Entering such a number proves that the user is an authorized user.

The check of user identification as described above can maintain security even when someone sneakily picks up a number that a user enters. This is because the number that the user enters is not a fixed code such as a pin code. This scheme thus provides higher security.

In this scheme, however, a user needs to remember both the registered formula and the key

1 number, and to calculate a required number in head.
This poses great burden on the part of the user.

 Further, the system also bears the burden in
that the system needs to store in memory the registered
5 formula and the registered key number for each user.
This requires a large memory size.

 Accordingly, there is a need for a scheme
which can achieve high security without imposing undue
burden on users or on the system.

10

SUMMARY OF THE INVENTION

 Accordingly, it is a general object of the
present invention to provide a scheme which satisfies
the need described above.

15 It is another and more specific object of the
present invention to provide a scheme which can achieve
high security without imposing undue burden on users or
on the system.

 In order to achieve the above objects
20 according to the present invention, a device for
checking user identification includes a calculation
unit which calculates a check value by applying a user-
specific formula to at least one randomly generated
number, and a matching unit which checks if the check
25 value matches a user-entered value that is entered by a
user in response to said at least one randomly
generated number presented to the user.

 In the device described above, the random
number is presented to the user, and the check value is
30 obtained from the random number and the user-specific
formula. Then, the check value is compared with the
user-entered value that is entered by the user in
response to the random number presented to the user. A
match in the comparison indicates that the user is
35 authorized. This device insures high-level security
since secrecy of the user-specific formula is
maintained even when someone surreptitiously picks up

1 the number entered by the user.

Moreover, the user needs to remember only his/her user-specific formula and nothing else. Likewise, the system needs to store only a formula for
5 each user. High-level security is thus achieved without imposing excessive burden on the user or on the system.

Other objects and further features of the present invention will be apparent from the following
10 detailed description when read in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig.1 is a block diagram of a user-
15 identification check system according to a principle of the present invention;

Fig.2 is an illustrative drawing showing an example of a computer which implements a user-
identification check device of Fig.1;

20 Fig.3 is a block diagram of an information processing device which implements user-identification check according to an embodiment of the present invention;

Fig.4 is an illustrative drawing showing an
25 example of identification-check data stored in an identification-check-data storage unit of Fig.3;

Fig.5 is a flowchart of a process of registering a password logic performed by an
identification-check-data control unit of Fig.3;

30 Fig.6 is a flowchart of a process of updating a password logic performed by the identification-check-data control unit;

Figs.7A and 7B is a flowchart of a process of checking user identification performed by an
35 identification-check unit of Fig.3;

Fig.8 is an illustrative drawing showing an example of a password-logic-registration window;

1 Fig.9 is an illustrative drawing showing an
example of a password input window;

 Fig.10 is an illustrative drawing of a user-
identification check system according to another
5 embodiment of the present invention;

 Fig.11 is a flowchart of a process of
registering a password logic performed by an
interaction unit of Fig.10;

 Fig.12 is a flowchart of a process of
10 registering a password logic performed by an
identification-check-data control unit of Fig.10;

 Figs.13A and 13B is a flowchart of a process
of updating a password logic performed by the
interaction unit;

15 Figs.14A and 14B is a flowchart of a process
of updating a password logic performed by the
identification-check-data control unit;

 Fig.15 is a flowchart of a process of
checking user identification performed by the
20 interaction unit;

 Fig.16 is a flowchart of a process of
checking user identification performed by the
identification-check unit of Fig.10;

 Fig.17 is an illustrative drawing of a user-
25 identificatin-check system utilizing a user-
identification-check card according to the present
invention; and

 Figs.18A and 18B are a flowchart of a process
performed by a card-identification-check unit of Fig.17
30 when checking user identification by use of a card.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

 In the following, a principle and embodiments
of the present invention will be described with
35 reference to the accompanying drawings.

 Fig.1 is a block diagram of a user-
identification check system according to a principle of

00441031-11599

1 the present invention.

In Fig.1, a user-identification check device 1 performs a process of checking user identification. A terminal 2 is provided for the user-identification check device 1, and provides a user with a means to interact with the user-identification check device 1.

The user-identification check device 1 according to the present invention includes a control-data unit 10, a registration/updating unit 11, a random-number generating unit 12, a selection unit 13, a calculation unit 14, and a matching unit 15.

The control-data unit 10 keeps correspondences between user IDs and formulas associated with the users. Depending on a user, a series of digits is provided in place of a formula. The registration/updating unit 11 is used for registering or updating formulas in the control-data unit 10. The random-number generating unit 12 generates a series of a predetermined number of random digits (or one digit), and presents the series of random digits to a user.

The selection unit 13 selects a formula corresponding to an indicated user ID from the control data of the control-data unit 10. The calculation unit 14 calculates a number to be used for the identification purpose by using the random number (i.e., the series of random digits) generated by the random-number generating unit 12 and the formula selected by the selection unit 13. The matching unit 15 checks whether a number entered by a user in response to the presentation of the random digits matches the number calculated by the calculation unit 14. A match indicates that the user is authorized.

The functions of the user-identification check device 1 are normally implemented via software programs running on a computer.

Fig.2 is an illustrative drawing showing an

1 example of a computer which implements the user-
identification check device 1.

A computer 100 of Fig.2 includes a CPU 101, a
RAM 102, a ROM 103, a MODEM 104, a memory drive 105, an
5 auxiliary memory 106, and a bus 107 connecting these
elements together. A user-identification program is
stored in a remote storage 108 connected to the modem
104 via a communication line, and/or is stored in a
memory medium 109 such as a floppy disk, a CD-ROM, a
10 memory card, or the like. The user-identification
program is loaded to the computer 100 from the remote
storage 108 via the modem 104 or from the memory medium
109 via the memory drive 105. The loaded program may
be stored in the auxiliary memory 106 for subsequent
15 loading to the RAM 102, or may be directly stored in
the RAM 102. The CPU 101 executes the user-
identification program stored in the RAM 102 by using
an available memory space of the RAM 102 as its work
area, and performs functions of the
20 registration/updating unit 11, the random-number
generating unit 12, the selection unit 13, the
calculation unit 14, and the matching unit 15. The
auxiliary memory 106 serves as the control-data unit
10. Further, the ROM 103 stores programs therein for
25 controlling basic operations of the computer 100.

Not only the configuration of Fig.1 may be
implemented on the computer 100 of Fig.2, but also
other configurations of embodiments, which will be
described later, may be implemented on a computer such
30 as the computer 100 shown in Fig.2.

With reference to Fig.1 again, the
registration/updating unit 11 receives a formula (or a
series of digits) entered in the terminal 2, and
registers the formula and a relevant user ID as a pair
35 in the control-data unit 10. When there is a request
for updating a formula registered in the control-data
unit 10, the registration/updating unit 11 receives a

5 In this manner, through operations of the
registration/updating unit 11, the control-data unit 10
keeps correspondences between the user IDs and the
formulas (or digits) associated with users.

In response, the calculation unit 14 calculates a number for the user-identification purpose by referring to the random number generated by the random-number generating unit 12 and the formula selected by the selection unit 13. The matching unit 15 checks whether a number entered in the terminal 2 in response to the presentation of the random number matches the number calculated by the calculation unit 14, thereby checking the identification of the user.

A time-dependent variable such as that which changes from 1 to 12 according to the current month may
35 be included in the formula. In such a case, the calculation unit 14 uses the time-dependent variable and the random number generated by the random-number

1 generating unit 12 to calculate a number for the
identification purpose based on the formula selected by
the selection unit 13.

The time-dependent variable may be created in
5 various manners to indicate a time of user
identification. That is, it may be created by
combining part or all of the year and date
(yyyy.mm.dd), time (hh.mm.ss), AM/PM (e.g., AM=0,
PM=1), day (e.g., Monday=1, Tuesday=2, and so on).

10 As described above, the user-identification
check device 1 registers formulas associated with
users, and presents a generated random number to a
user. A user enters a number in response to the
presentation of the random number. The user-
15 identification check device 1 checks if the user-
entered number matches a number calculated from a
selected formula and the generated random number,
thereby checking if the user is authorized. This
configuration maintains security even when someone
20 surreptitiously picks up a number entered by a user.

When this system is used in a network
environment, it is made sure that the formulas
associated with users are not sent through the network.
This insures higher security than a conventional system
25 where pin numbers need to be sent through the network.

The user-identification check scheme of
Japanese Patent Laid-open Application No. 63-170764 as
previously described requires a user to remember both a
formula and a key number. On the other hand, the
30 present invention requires the user to remember only
his/her formula. Further, the scheme of the above
document demands that the system store formulas and key
numbers in its memory. The present invention, on the
other hand, suffice only if the system stores formulas
35 in its memory. The present invention thus provides
high security without imposing undue burden on the
users or on the system.

1 Further, according to the present invention,
a user-identification-check card may be provided for a
user, and stores therein the user's formula. This
configuration also achieves high security.

5 In the following, embodiments of the present
invention will be described with the accompanying
drawings.

Fig.3 is a block diagram of an information
processing device which implements user-identification
10 check according to an embodiment of the present
invention.

An information processing device 20 of Fig.3
includes a display unit 21 such as a CRT, an input unit
22 such as a keyboard and a mouse, an identification-
15 check-data storage unit 23, an identification-check-
data control unit 24, and an identification-check unit
25. The identification-check-data storage unit 23
stores therein data that is necessary for user-
identification check. The identification-check-data
20 control unit 24 attends to registration and updating of
the identification-check data stored in the
identification-check-data storage unit 23, and is
implemented via a program installed through a floppy
disk, a communication line, or the like. The
25 identification-check unit 25 performs a user-
identification-check process by referring to the
identification-check data stored in the identification-
check-data storage unit 23, and is implemented via a
program installed through a floppy disk, a
30 communication line, or the like.

Fig.4 is an illustrative drawing showing an
example of the identification-check data stored in the
identification-check-data storage unit 23.

As shown in the figure, the identification-
35 check-data storage unit 23 stores paired user IDs and
password logics where the password logics are
registered by respective users. Depending on user

1 preference, a given password logic may be a simple
personal identification number.

The password logics generally define
formulas, which are applied to random digits generated
5 by the identification-check unit 25. In the example
shown in Fig.4, a user having a user ID "000005"
registered a password logic that calculates "A-B" when
a 4-digit random number ABCD is presented. On the
other hand, a user having a user ID "000004" registered
10 a pin code "5348" rather than a formula, so that this
pin code is stored in the identification-check-data
storage unit 23.

In the example of Fig.4, password logics are
shown by using a general form of formula representation
15 for the sake of simplicity. In practice, however, the
password logics may be stored by using a special form
of representation such as the Reversed Polish Notation.

According to the Reversed Polish Notation,
the formulas shown in Fig.4 are represented as follows:

20 $10 \times A \rightarrow 10A^*$;
 $A \times A \rightarrow AA^*$;
 $A \div B \rightarrow AB/$;
 $A - B \rightarrow AB-$;
 $(B-A) + C \rightarrow BA-C+$; and
25 $((A - B) \times 5) \div 2 \rightarrow AB-5*2/$.

Use of such a form of representation makes it more
difficult to decipher codes, thereby enhancing level of
security.

Fig.5 is a flowchart of a process of
30 registering a password logic performed by the
identification-check-data control unit 24.

At a step ST1, upon a request for
registration of a password logic, the identification-
check-data control unit 24 displays a password-logic-
35 registration window on the display unit 21. Fig.8 is
an illustrative drawing showing an example of the
password-logic-registration window.

1 At a step ST2, a user enters a user ID in the
password-logic-registration window.

 At a step ST3, the user enters a password
logic in the password-logic-registration window.

5 As will be described later in detail, the
identification-check unit 25 generates a 4-digit random
number ABCD (each digit ranges from 0 to 9). With
respect to this random number, a user defines his/her
own formula that is to be applied to the four digits of
10 the random number. Here, the user does not have to use
each one of the four digits, and is allowed to include
parentheses in his/her formula. The identification-
check-data control unit 24 receives the user-defined
password logic, and registers it. If the user wishes
15 to use a conventional pin code, the user simply enters
a pin code comprised of four digits. The
identification-check-data control unit 24 then
registers this pin code.

 At a step ST4, a check is made as to whether
20 the user operates an END button (i.e., a button for
finishing a registration process). If a CANCEL button
is operated, the procedure comes to an end. If the END
button is operated, the procedure goes to a step ST5.

 At the step ST5, a check is made as to
25 whether the user has another password logic already
registered in the identification-check-data storage
unit 23.

 If the step ST5 finds that another password
logic is already in place in the identification-check-
30 data storage unit 23, at a step ST6, the
identification-check-data control unit 24 displays a
message indicating presence of an already registered
password logic on the display unit 21, thereby
informing the user that the password logic entered at
35 the step ST3 is not registered. The procedure comes to
an end after the step ST6.

 If the step ST5 finds that the user has no

1 password logic.

If the step ST6 finds that the two password logics match, the procedure goes to a step ST7, where the user enters a new password logic.

5 At a step ST8, a check is made as to whether the user operates an END button (i.e., a button for finishing a registration process). If a CANCEL button is operated, the procedure comes to an end. If the END button is operated, the procedure goes to a step ST9.

10 At the step ST9, the identification-check-data control unit 24 updates the old password logic with the new password logic in the identification-check-data storage unit 23. The procedure then comes to an end.

15 In this manner, the identification-check-data control unit 24 updates a password logic stored in the identification-check-data storage unit 23 upon a user request for updating a password logic only if the user knows the old password logic stored in the identification-check-data storage unit 23.

20 According to the flowcharts of Figs.5 and 6, the identification-check-data storage unit 23 registers paired user IDs and password logics (or pin numbers) in the identification-check-data storage unit 23.

25 Figs.7A and 7B is a flowchart of a process of checking user identification performed by the identification-check unit 25.

At a step ST1, upon a user request for identification check, the identification-check unit 25 generates a four-digit random number as represented by ABCD.

30 At a step ST2, the identification-check unit 25 displays a password-input window on the display unit 21, and presents the generated random number in the window. If a random number "4361" is generated, for example, this number is presented to a user. Fig.9 is an illustrative drawing showing an example of the

1 password input window.

At a step ST3, the user enters a user ID and a password.

The password entered by the user is
5 calculated by applying the password logic registered in the identification-check-data storage unit 23 to the digits A, B, C, and D of the random number generated by the identification-check unit 25. If a random number "4361" is generated by the identification-check unit
10 25, and if the user has a registered password logic "A+B+C+D", the user calculates "4+3+6+1" to obtain a password "14". The user then enters the obtained password in the password-input window.

If a password logic has a division operation
15 that has "0" as its denominator, the identification-check unit 25 substitutes "0" for the result of the division operation. The user has to follow this rule to obtain a password. Further, if a password logic has a division operation that produces a remainder, the
20 identification-check unit 25 discards digits below a decimal point. The user has to obey this rule when obtaining a password. Moreover, the identification-check unit 25 obtains an absolute value of a result of the password logic operation when the result of the
25 password logic operation becomes negative. The user needs to respect this rule as well. The rules described above are merely an example, and other rules may be set forth when appropriate.

When the user has a pin code registered in
30 the identification-check-data storage unit 23, the user enters the pin code as a password in the password-input window.

At a step ST4, a check is made as to whether the user ID entered at the step ST3 is found as a
35 registered user ID in the identification-check-data storage unit 23.

If the step ST4 finds that the user ID is a

1 registered user ID, at a step ST5, a password logic
registered for the user is obtained by referring to the
identification-check-data storage unit 23.

At a step ST6, the random number generated at
5 the step ST1 is broken down into four separate digits
A, B, C, and D.

At a step ST7, the four digits are inserted
into the password logic obtained at the step ST5 to
produce a value corresponding to the password entered
10 by the user.

In so doing, the identification-check unit 25
substitutes "0" for a result of a division operation if
the division operation in the password logic has "0" as
its denominator, and discards digits below a decimal
15 point if a division operation in the password logic
produces a remainder. Moreover, the identification-
check unit 25 obtains an absolute value of a result of
the password logic operation when the result of the
password logic operation becomes negative, and outputs
20 a pin code if the pin code is defined in place of a
password logic.

At a step ST8, the password entered at the
step ST3 is compared with the value obtained at the
step ST7.

25 At a step ST9, a check is made as to whether
the comparison indicates a match. If there is a match,
the procedure goes to a step ST10, where the
identification-check unit 25 outputs a signal (data)
indicative of authorization of the user. In response,
30 a program for predetermined business processing starts
operation thereof. This ends the procedure.

If the step ST4 finds that the entered user
ID is not a registered user ID, or if the step ST9
finds that the entered password does not match the
35 obtained value, the procedure goes to a step ST11 of
Fig.7B.

At the step ST11, a check is made as to

1 whether the user-identification check has been
attempted a predetermined number of times. If the
predetermined number of attempts have been made, the
procedure goes to a step ST12, where the
5 identification-check unit 25 displays a message
indicating a wrong user identification on the display
unit 21. This ends the procedure.

If the step ST11 finds that the user-
identification check has not been attempted the
10 predetermined number of times, the procedure goes to a
step ST13, where a count of the number of attempts is
increased by one. Then, the procedure goes back to the
step ST1 to repeat the user-identification-check
process as described above.

15 In this manner, the identification-check unit
25, upon a user request for identification check,
obtains a value by using a user-defined password logic
registered in the identification-check-data storage
unit 23 and a random number, and compares the obtained
20 value with a password that is entered by the user in
response to the random number presented to the user,
thereby making a proper user-identification check.

Use of such user-identification check insures
high-level security even if someone surreptitiously
25 picks up a number that the user enters. The user needs
to remember only his/her password logic and nothing
else. Likewise, the system needs to store only a
password logic for each user. High-level security is
thus achieved without imposing excessive burden on the
30 user or on the system.

Further, the embodiment described above is
applicable to a case where conventional pin codes are
used as an option. In this manner, this embodiment can
cope with various user preferences including use of a
35 pin code if the user so wishes.

Fig.10 is an illustrative drawing of a user-
identification check system according to another

1 embodiment of the present invention.

 In this embodiment, the present invention is applied to a distribution-management system operating in a network environment.

5 The distribution-management system of Fig.10 includes an identification-check server 30, a plurality of distribution terminals 40, and a network 50 connecting between the identification-check server 30 and the distribution terminals 40. The identification-check server 30 attends to user-identification check.
10 The distribution terminals 40 are provided at the end of distributors.

 The identification-check server 30 includes an identification-check-data storage unit 31, an
15 identification-check-data control unit 32, and an identification-check unit 33. The identification-check-data storage unit 31 stores data in the same format as the identification-check-data storage unit 23 of Fig.3. The identification-check-
20 data control unit 32 attends to registration and updating of the identification-check data stored in the identification-check-data storage unit 31, and may be implemented as a software program installed from a floppy disk, CD-ROM, or the like, or installed from a
25 remote storage via a communication line. The identification-check unit 33 performs a user-identification-check process by referring to the identification-check data stored in the identification-check-data storage unit 31, and may be implemented as a
30 software program installed from a floppy disk, CD-ROM, or the like, or installed from a remote storage via a communication line.

 A distribution terminal 40 includes a display unit 41 such as a CRT, an input unit 42 such as a
35 keyboard and a mouse, and an interaction unit 43. The interaction unit 43 provides a user with a means to interact with the system, and may be implemented as a

1 software program installed from a floppy disk, CD-ROM,
or the like, or installed from a remote storage via a
communication line.

Fig.11 is a flowchart of a process of
5 registering a password logic performed by the
interaction unit 43.

At a step ST1, upon a request for
registration of a password logic, the interaction unit
43 of the distribution terminal 40 displays a password-
10 logic-registration window on the display unit 41 as
shown in Fig.8.

At a step ST2, a user enters a user ID in the
password-logic-registration window.

At a step ST3, a user enters a user-defined
15 password logic in the password-logic-registration
window. This password logic is of the same type as
that used in the previous embodiment.

At a step ST4, a check is made as to whether
the user operates an END button (i.e., a button for
20 activating a registration process). If a CANCEL button
is operated, the procedure comes to an end. If the END
button is operated, the procedure goes to a step ST5.

At the step ST5, the interaction unit 43
sends the entered user ID and password logic to the
25 identification-check-data control unit 32 of the
identification-check server 30.

As will be described later in detail, the
identification-check-data control unit 32 returns a
message in response to the transmission of the user ID
30 and the password logic, and the message indicates
whether registration of the password logic is
completed.

At a step ST6, a check is made as to whether
this return message is received from the
35 identification-check-data control unit 32. When the
message is received, the procedure goes to a step ST7.

At the step ST7, a check is made as to

1 whether the message indicates that registration of the
password logic is completed.

If the step ST7 finds that registration of
the password logic is completed, the procedure comes to
5 an end. If the step ST7 finds that registration is not
completed, at a step ST8, the interaction unit 43
presents a message on the display unit 41 to indicate
that registration of the password logic has failed.
Then, the procedure comes to an end.

10 Fig.12 is a flowchart of a process of
registering a password logic performed by the
identification-check-data control unit 32.

At a step ST1, upon a request by the
interaction unit 43 to register a password logic, the
15 identification-check-data control unit 32 of the
identification-check server 30 receives the user ID and
the password logic from the interaction unit 43.

At a step ST2, a check is made as to whether
a user indicated by the user ID has a password logic
20 already registered in the identification-check-data
storage unit 31. If there is an already registered
password logic, the procedure goes to a step ST3, where
the identification-check-data control unit 32 sends a
message to the interaction unit 43 to indicate that
25 registration of the password logic cannot be completed.
Then, the procedure comes to an end.

If the step ST2 finds that the user indicated
by the user ID does not have a password logic already
registered in the identification-check-data storage
30 unit 31, the procedure goes to a step ST4.

At the step ST4, the received password logic
and the received user ID are registered as a pair in
the identification-check-data storage unit 31.

At a step ST5, the identification-check-data
35 control unit 32 sends a message indicative of
completion of the registration to the interaction unit
43.

1 In this manner, the interaction unit 43 and
the identification-check-data control unit 32 interact
with each other via the network 50 when a user requests
registration of a password logic, and collaboratively
5 register the user-defined password logic in the
identification-check-data storage unit 31.

Figs.13A and 13B is a flowchart of a process
of updating a password logic performed by the
interaction unit 43.

10 At a step ST1, upon a user request for
updating a password logic, the interaction unit 43 of
the distribution terminal 40 displays a password-logic-
registration window on the display unit 41 as shown in
Fig.8.

15 At a step ST2, the user enters a user ID in
the password-logic-registration window.

At a step ST3, the user enters an old
password logic in the password-logic-registration
window.

20 At a step ST4, a check is made as to whether
the user operates an OK button (i.e., a button for
entering the old password logic). If the OK button is
operated, the procedure goes to a step ST5.

At the step ST5, the interaction unit 43
25 sends the entered user ID and the entered old password
logic to the identification-check-data control unit 32.

As will be described later in detail, the
identification-check-data control unit 32 returns a
message in response to the transmission of the user ID
30 and the old password logic, and the message indicates
whether updating of the password logic is acceptable.

At a step ST6, a check is made as to whether
this return message is received from the
identification-check-data control unit 32. When the
35 message is received, the procedure goes to a step ST7.

At the step ST7, a check is made as to
whether the message indicates that updating of the

1 password logic is acceptable.

If the step ST7 finds that updating of the password logic is unacceptable, the procedure goes to a step ST8, where a message is presented on the display unit 41 to indicate that updating of the password logic is not acceptable. Then, the procedure comes to an end.

If the step ST7 finds that updating of the password logic is acceptable, the procedure goes to a step ST9, where the user enters a new password logic for the updating purpose.

At a step ST10 of Fig.13B, a check is made as to whether the user operates an END button (i.e., a button for activating a registration process). If a CANCEL button is operated, the procedure comes to an end. If the END button is operated, the procedure goes to a step ST11.

At the step ST11, the interaction unit 43 sends the user ID and the new password logic entered at the step ST9 to the identification-check-data control unit 32.

As will be described later in detail, the identification-check-data control unit 32 returns a message in response to the transmission of the user ID and the new password logic, and the message indicates whether registration of the new password logic is completed.

At a step ST12, a check is made as to whether this return message is received from the identification-check-data control unit 32. When the message is returned, the procedure comes to an end.

Figs.14A and 14B is a flowchart of a process of updating a password logic performed by the identification-check-data control unit 32.

At a step ST1, upon a request by the interaction unit 43 to update a password logic, the identification-check-data control unit 32 of the

1 identification-check server 30 receives the user ID and
the old password logic from the interaction unit 43.

At a step ST2, the identification-check-data
control unit 32 refers to the identification-check-data
5 storage unit 31 to obtain a password logic
corresponding to the received user ID.

At a step ST3, a check is made as to whether
the password logic obtained at the step ST2 matches the
password logic received at the step ST1. If there is
10 no match, the procedure goes to a step ST4, where a
message indicative of denial of the updating request is
send to the interaction unit 43. The procedure comes
to an end.

If the step ST3 finds that the two password
15 logics match, the procedure goes to a step ST5, where a
message indicative of acceptance of the updating
request is sent to the interaction unit 43.

As previously described, the interaction unit
43 responds to the message indicative of acceptance of
20 the updating request sent from the
identification-check-data control unit 32 by sending
the user ID and a new password logic.

At a step ST6, a check is made as to whether
the user ID and a new password logic are received from
25 the interaction unit 43. When they are received, the
procedure goes to a step ST7 of Fig.14B.

At the step ST7 of Fig.14B, the
identification-check-data control unit 32 updates the
old password logic indicated by the received user ID
30 with the received new password logic in the
identification-check-data storage unit 31.

At a step ST8, the identification-check-data
control unit 32 sends a message indicating completion
of a password-logic updating process to the interaction
35 unit 43. This ends the procedure.

In this manner, the interaction unit 43 and
the identification-check-data control unit 32 interact

1 with each other via the network 50 when a user requests
updating of a password logic, and collaboratively
update the password logic in the identification-check-
data storage unit 31 only if the user knows the old
5 password logic.

Based on the procedures shown as flowcharts
in Fig.11 through Figs.14A and 14B, user IDs and
password logics (or pin codes) associated with the user
IDs are stored in the identification-check-data storage
10 unit 31 of the identification-check server 30.

Based on this identification-check data
stored in the identification-check-data storage unit
31, the interaction unit 43 and the identification-
check unit 33 interact with each other via the network
15 50 to perform a user-identification check when a user
requests a check of user identification.

Fig.15 is a flowchart of a process of
checking user identification performed by the
interaction unit 43.

20 At a step ST1, upon a user request for
identification check, the interaction unit 43 of the
distribution terminal 40 generates a four-digit random
number as represented by ABCD.

At a step ST2, the identification-check unit
25 25 displays a password-input window on the display unit
21 as shown in Fig.9, and presents the generated random
number in the window. If a random number "4361" is
generated, for example, this number is presented to a
user.

30 As will be described later, the random number
generated at this step does not have to be a four-digit
random number, but can be comprised of only one digit,
two digits, or three digits. By the same token, the
random number may be comprised of a larger number of
35 digits more than four.

At a step ST3, the user enters a user ID and
a password.

1 The password entered by the user is
calculated by applying the password logic registered in
the identification-check-data storage unit 31 to the
digits A, B, C, and D of the random number generated by
5 the interaction unit 43. If a password logic has a
division operation that has "0" as its denominator, the
user obtains the password by substituting "0" for the
result of the division operation. Further, if a
password logic has a division operation that produces a
10 remainder, the user obtains the password by discarding
digits below a decimal point. Moreover, the user
obtains the password by calculating an absolute value
of a result of the password logic operation when the
result of the password logic operation becomes
15 negative. When the user has a pin code registered in
the identification-check-data storage unit 31, the user
enters the pin code as the password in the password-
input window.

20 At a step ST4, the interaction unit 43 sends
the random number generated at the step ST1 and the
user ID and password entered at the step ST3 to the
identification-check unit 33.

 As will be described later in detail, the
identification-check unit 33 returns a message in
25 response to the transmission of the random number, the
user ID, and the password, and the message indicates
whether the user is authorized by entering the
password.

30 At a step ST5, a check is made as to whether
this return message is received from the
identification-check unit 33. When the message is
received, the procedure goes to a step ST6.

 At the step ST6, a check is made as to
whether the return message indicates that user
35 authorization is completed.

 If the step ST6 finds that the message
received from the identification-check unit 33

1 indicates completion of user authorization, at a step
ST7, the interaction unit 43 outputs a signal (data)
indicative of authorization of the user. In response,
a program for business processing starts operation
5 thereof. This ends the procedure.

If the step ST6 finds that the message
received from the identification-check unit 33
indicates denial of user authorization, the procedure
goes to a step ST8.

10 At the step ST8, a check is made as to
whether the user-identification check has been
attempted a predetermined number of times. If the
predetermined number of attempts have been made, the
procedure goes to a step ST9, where the interaction
15 unit 43 displays a message indicating a wrong user
identification on the display unit 41. This ends the
procedure.

If the step ST8 finds that the user-
identification check has not been attempted the
20 predetermined number of times, the procedure goes to a
step ST10, where a count of the number of attempts is
increased by one. Then, the procedure goes back to the
step ST1 to repeat the user-identification-check
process as described above.

25 Fig.16 is a flowchart of a process of
checking user identification performed by the
identification-check unit 33.

At a step ST1, upon a request by the
interaction unit 43 to check user identification, the
30 identification-check unit 33 of the identification-
check server 30 receives the random number, the user
ID, and the password from the interaction unit 43.

At a step ST2, a check is made as to whether
the received user ID is found as a registered user ID
35 in the identification-check-data storage unit 31.

If the step ST2 finds that the user ID is a
registered user ID, at a step ST3, a password logic

1 the procedure.

In the manner as described in conjunction with Fig.15 and Fig.16, when a user requests a check of user identification, the interaction unit 43 and the
5 identification-check unit 33 interact with each other via the network 50. Through the interaction, a value is obtained from a random number and a password logic registered in the identification-check-data control unit 32, and is compared with a password that is
10 entered by the user in response to the random number presented to the user. This achieves a proper user-identification check.

Use of such user-identification check insures high-level security even if someone surreptitiously
15 picks up a number that the user enters. The user needs to remember only his/her password logic and nothing else. Likewise, the system needs to store only a password logic for each user. High-level security is thus achieved without imposing excessive burden on the
20 user or on the system.

The password logic, which is equivalent to a personal identification code, is not transmitted through the network 50, except when the password logic is registered in the identification-check-data storage
25 unit 31. This decreases a chance of someone picking up the password logic from the network 50, thereby achieving high-level security.

In the procedures of Fig.15 and Fig.16, the interaction unit 43 generates a random number.
30 Alternatively, the identification-check unit 33 may generate a random number, and send it to the interaction unit 43.

As described above, the present invention registers a user-defined password logic, and generates
35 a random number to be presented to a user. The user enters a password (value) in response to the presented random number. Then, the system generates a value from

1 the random number and the user-defined password logic,
and checks if the user-entered password matches the
system-generated value, thereby checking a user
identification.

5 According to this principle, the present
invention may use a magnetic stripe card or an IC card
as a user-identification-check card, which record
therein a user-defined password logic instead of a pin
code.

10 A conventional user-identification-check card
such as a magnet stripe card or an IC card records
therein a user ID and a pin code. In contrast, the
user-identification-check card according to the present
invention records therein a user ID and a user-defined
15 password logic.

Fig.17 is an illustrative drawing of a user-
identification-check system utilizing a user-
identification-check card according to the present
invention.

20 As shown in the figure, an IC card 60 of the
present invention includes a memory unit 600 and a
random-number generation unit 601. The memory unit 600
stores therein a user ID and a user-defined password
logic.

25 The IC card 60 is inserted into an IC-card
reader 70 connected to the distribution terminal 40.
The distribution terminal 40 includes a card-
identification-check unit 44 for performing a user-
identification check by using the password logic
30 recorded in the IC card 60.

Figs.18A and 18B are a flowchart of a process
performed by the card-identification-check unit 44 when
checking user identification by use of a card. With
reference to these figures, a check of user
35 identification based on the IC card 60 will be
described below.

At a step ST1, upon a request for user-

1 identification check with respect to the IC card 60,
the card-identification-check unit 44 of the
distribution terminal 40 reads a user ID and a password
logic from the IC card 60.

5 At a step ST2, the card-identification-check
unit 44 receives a random number that is generated by
the random-number generation unit 601 of the IC card
60.

10 At a step ST3, the card-identification-check
unit 44 displays a password-input window as shown in
Fig.9, and presents the random number to the user. For
example, a random number "4361" is generated and
presented in the password-input window.

15 At a step ST4, the user enters a password in
the password-input window.

20 The user calculates the password by applying
the password logic recorded in the IC card 60 to the
digits A, B, C, and D of the random number generated by
the random-number generation unit 601. If a password
logic has a division operation that has "0" as its
denominator, the user obtains the password by
substituting "0" for the result of the division
operation. Further, if a password logic has a division
operation that produces a remainder, the user obtains
25 the password by discarding digits below a decimal
point. Moreover, the user obtains the password by
calculating an absolute value of a result of the
password logic operation when the result of the
password logic operation becomes negative. When the
30 user has a pin code recorded in the IC card 60, the
user enters the pin code as the password in the
password-input window.

35 At a step ST5, the random number received at
the step ST2 is broken down into four separate digits
A, B, C, and D.

At a step ST6, the four digits are inserted
into the password logic obtained at the step ST1 to

1 produce a value corresponding to the password entered
by the user.

At a step ST7, the password entered at the
step ST4 is compared with the value obtained at the
5 step ST6.

At a step ST9, a check is made as to whether
the comparison indicates a match. If there is a match,
the procedure goes to a step ST9, where the card-
identification-check unit 44 outputs a signal (data)
10 indicative of authorization of the user. In response,
a program for business processing starts operation
thereof. This ends the procedure.

If the step ST8 finds that the entered
password does not match the obtained value, the
15 procedure goes to a step ST10.

At the step ST10, a check is made as to
whether the user-identification check has been
attempted a predetermined number of times. If the
predetermined number of attempts have been made, the
20 procedure goes to a step ST11 of Fig.18B, where the
card-identification-check unit 44 displays a message
indicating a wrong user identification on the display
unit 41. This ends the procedure.

If the step ST10 finds that the user-
25 identification check has not been attempted the
predetermined number of times, the procedure goes to a
step ST12, where a count of the number of attempts is
increased by one. Then, the procedure goes back to the
step ST1 to repeat the user-identification-check
30 process as described above.

In this manner, the configuration described
above utilizes a user-identification-check card such as
a magnetic stripe card or an IC card which records
therein a user-defined password logic. This
35 configuration obtains a value from a random number and
a user-defined password logic recorded in the user-
identification-check card, and compares the obtained

1 value with a password that is entered by the user in
response to the random number presented to the user.
This achieves a proper user-identification check.

Such a configuration insures high-level
5 security since secrecy of password logic is maintained
even when someone surreptitiously picks up a number
that the user enters.

In the configuration of Fig.17, the IC card
60 is equipped with the random-number generation unit
10 601. Alternatively, a mechanism for generating a
random number may be provided in the card-
identification-check unit 44.

In the embodiments described above, a
password logic is applied to randomly generated digits.
15 In addition to such digits, variables that can be
uniquely determined by users or the system may be used
as well. Such variables include date information, time
information, etc.

For example, a variable ranging from 1 to 12
20 corresponding to respective months from January to
December may be used, and/or a variable ranging from 0
to 24 corresponding to 0:00 hours to 24:00 hours may be
employed. Such a variable may be incorporated in the
password logic in addition to random digits. For
25 example, a password logic may be represented as " $(A - B) + n$ " where n represents the variable as described
above.

As described hereinbefore, the prevent
invention registers a user-defined password logic, and
30 generates a random number to be presented to the user.
The present invention then obtains a value from the
random number and the user-defined password logic, and
compares the obtained value with a value that is
entered by the user in response to the random number
35 presented to the user. This achieves a proper user-
identification check. The present invention insures
high-level security since secrecy of password logic is

1 maintained even when someone surreptitiously picks up a
number entered by the user.

Further, the present invention makes it
possible to avoid transmission of a password logic over
5 a network. In a network environment, therefore, the
present invention offers a higher level of security
than a conventional system, which transmits a pin code
over the network.

The user needs to remember only his/her
10 password logic and nothing else. Likewise, the system
needs to store only a password logic for each user.
High-level security is thus achieved without imposing
excessive burden on the user or on the system.

Further, the present invention may utilize a
15 card provided for a user for the purpose of owner
identification, and this card records therein a user-
defined password logic rather than a pin code. This
configuration achieves higher level security than does
a conventional system.

Further, the present invention is not limited
20 to these embodiments, but various variations and
modifications may be made without departing from the
scope of the present invention.

The present application is based on Japanese
25 priority application No. 11-113058 filed on April 21,
1999, with the Japanese Patent Office, the entire
contents of which are hereby incorporated by reference.

30

35

1 WHAT IS CLAIMED IS

5

1. A device for checking user identification,
comprising:

 a calculation unit which calculates a check
value by applying a user-specific formula to at least
10 one randomly generated number; and

 a matching unit which checks if the check
value matches a user-entered value that is entered by a
user in response to said at least one randomly
generated number presented to the user.

15

 2. The device as claimed in claim 1, wherein
20 said calculation unit outputs a fixed number as the
check value if the user-specific formula consists of
the fixed number.

25

 3. The device as claimed in claim 1, wherein
the user-specific formula includes a variable that is
an indication of a time at which said calculation unit
30 calculates the check value.

35

 4. The device as claimed in claim 1, further
comprising:
 a control-data unit which stores therein user

1 IDs and user-specific formulas associated with
 respective user IDs;
 a selection unit which selects the user-
 specific formula from said control-data unit in
5 response to a user ID of said user; and
 a random-number generating unit which
 generates said at least one randomly generated number.

10

 5. The device as claimed in claim 4, further
 comprising a registration/updating unit which updates
 one of the user-specific formulas in the control data
15 unit with a user-entered formula only if a user
 entering the user-entered formula proves knowledge of
 said one of the user-specific formulas by entering said
 one of the user-specific formulas.

20

 6. A method of checking user identification,
 comprising the steps of:
25 calculating a check value by applying a user-
 specific formula to at least one randomly generated
 number; and
 checking if the check value matches a user-
 entered value that is entered by a user in response to
30 said at least one randomly generated number presented
 to the user.

35

 7. The method as claimed in claim 6, wherein
 said step of calculating a check value outputs a fixed

1 number as the check value if the user-specific formula
consists of the fixed number.

5

8. The method as claimed in claim 6, wherein
the user-specific formula includes a variable that is
an indication of a time at which said step of
10 calculating a check value calculates the check value.

15 9. The method as claimed in claim 6, further
comprising the steps of:
 storing user IDs and user-specific formulas
 associated with respective user IDs in a data storage;
 selecting the user-specific formula from the
20 data storage in response to a user ID of said user; and
 generating said at least one randomly
generated number.

25

10. The method as claimed in claim 9, further
comprising a step of updating one of the user-specific
formulas in the data storage with a user-entered
30 formula only if a user entering the user-entered
formula proves knowledge of said one of the user-
specific formulas by entering said one of the user-
specific formulas.

35

1 11. A computer-readable medium having a
program embodied therein for causing a computer to
check user identification, said program comprising:
 a calculation code unit which calculates a
5 check value by applying a user-specific formula to at
least one randomly generated number; and
 a matching code unit which checks if the
check value matches a user-entered value that is
entered by a user in response to said at least one
10 randomly generated number presented to the user.

15 12. The computer-readable medium as claimed
in claim 11, wherein said calculation code unit outputs
a fixed number as the check value if the user-specific
formula consists of the fixed number.

20

 13. The computer-readable medium as claimed
in claim 11, wherein the user-specific formula includes
25 a variable that is an indication of a time at which
said calculation code unit calculates the check value.

30

 14. The computer-readable medium as claimed
in claim 11, wherein said program further comprises:
 a registration/updating code unit which
stores user IDs and user-specific formulas associated
35 with respective user IDs in a data storage;
 a selection code unit which selects the user-
specific formula from said data storage in response to

1 a user ID of said user; and
 a random-number generating code unit which
 generates said at least one randomly generated number.

5

15 15. The computer-readable medium as claimed
in claim 14, wherein said registration/updating code
10 unit updates one of the user-specific formulas in the
data storage with a user-entered formula only if a user
entering the user-entered formula proves knowledge of
said one of the user-specific formulas by entering said
one of the user-specific formulas.

15

20

25

30

35

1 ABSTRACT OF THE DISCLOSURE

 A device for checking user identification
includes a calculation unit which calculates a check
value by applying a user-specific formula to a randomly
5 generated number, and a matching unit which checks if
the check value matches a user-entered value that is
entered by a user in response to the randomly generated
number presented to the user.

10

15

20

25

30

35

FIG. 1

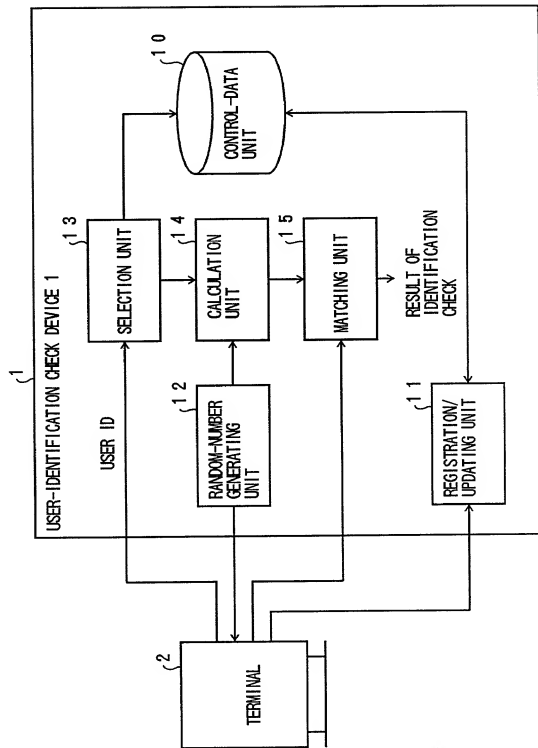


FIG. 2

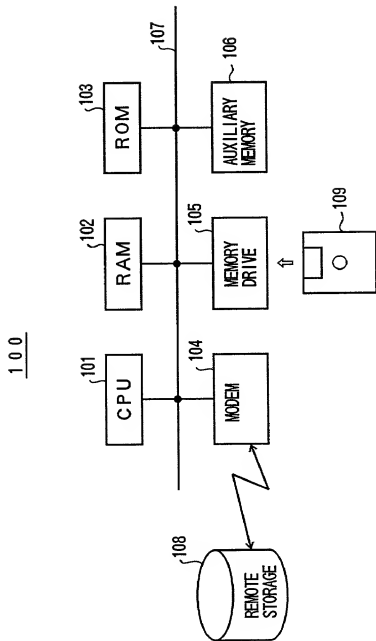


FIG. 3

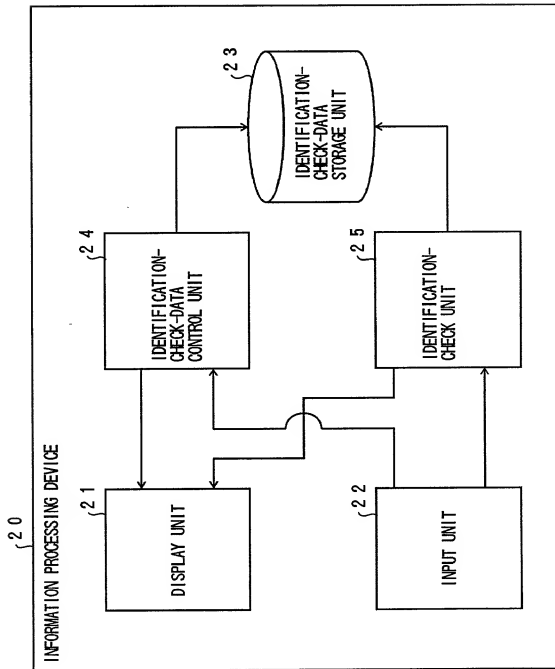


FIG. 4

23

USER ID	PASSWORD LOGIC
0 0 0 0 0 1	$10 \times A$
0 0 0 0 0 2	$A \times A$
0 0 0 0 0 3	$A \div B$
0 0 0 0 0 4	5 3 8 4
0 0 0 0 0 5	$A - B$
0 0 0 0 0 6	$(B - A) + C$
0 0 0 0 0 7	$((A - B) \times 5) \div 2$
.	.
.	.
.	.
.	.
.	.

FIG. 5

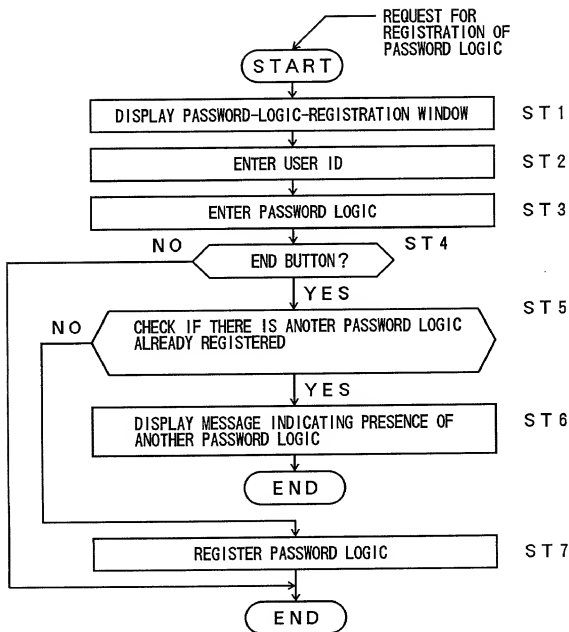


FIG. 6

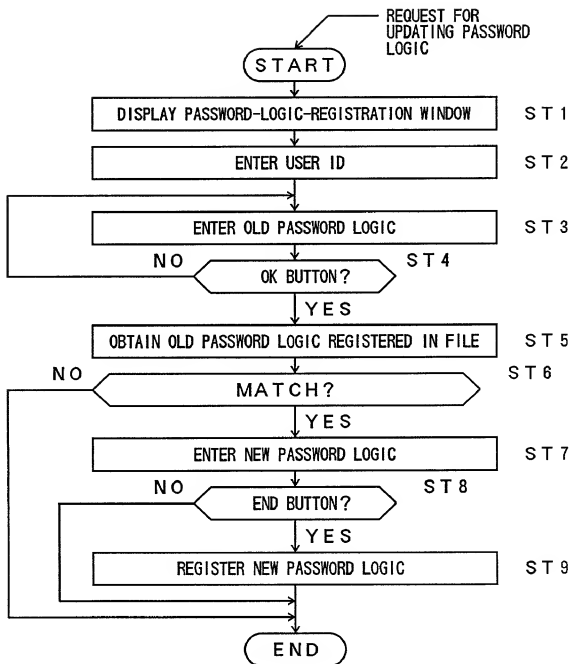


FIG. 7A

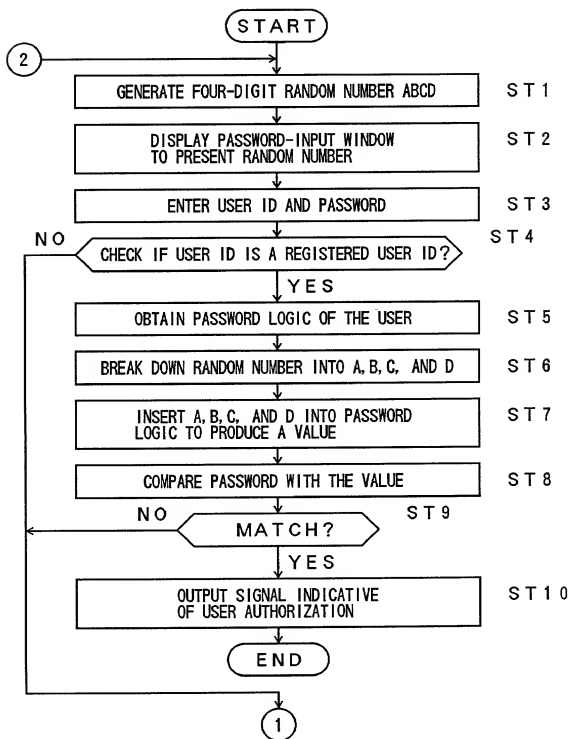


FIG. 7B

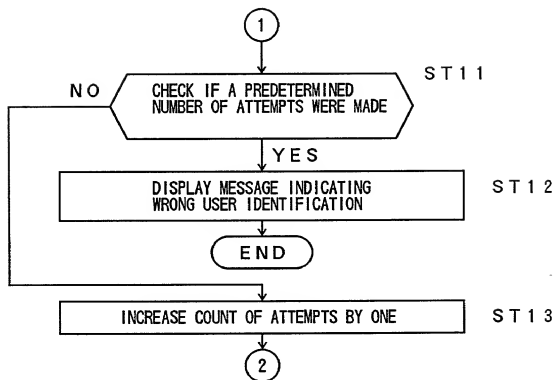


FIG. 8

PASSWORD LOGIC REGISTRATION		
USER ID	:	0 0 0 0 0 6
PASSWORD LOGIC	:	$(B - A) + C$
<div>O K CANCEL END</div>		

FIG. 9

ENTER PASSWORD

USER ID

:

0 0 0 0 0 1

PRESENTED NUMBER

:

4 3 6 1

PASSWORD

:

**

O K

CANCEL

END

FIG. 10

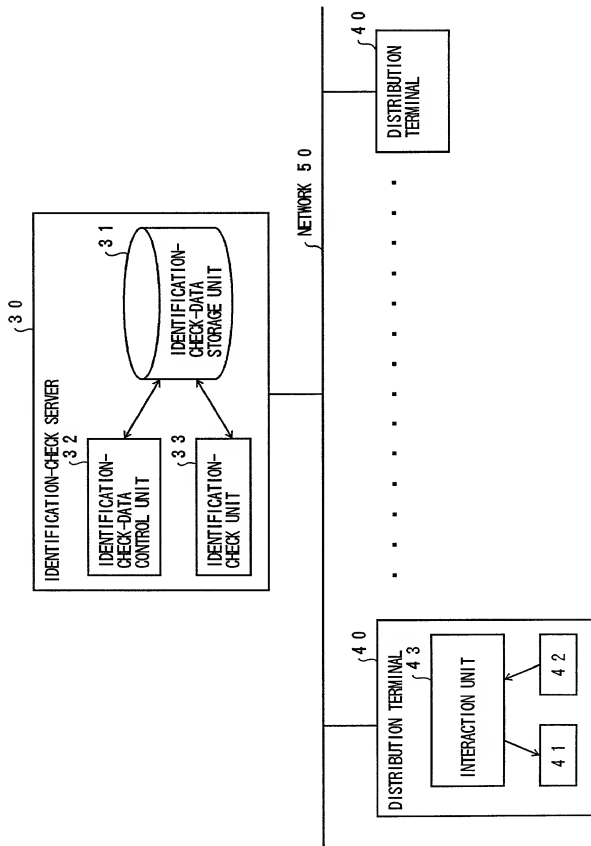


FIG. 11

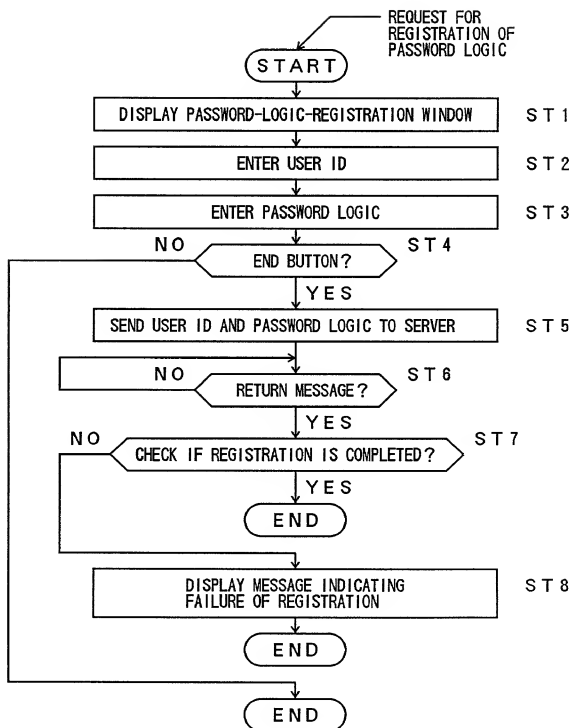


FIG. 12

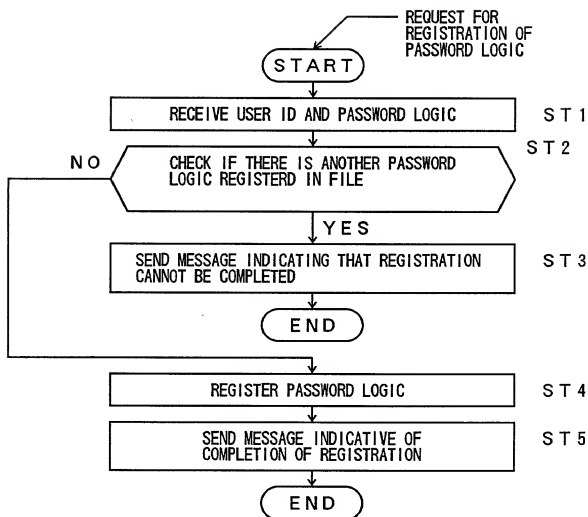


FIG. 13A

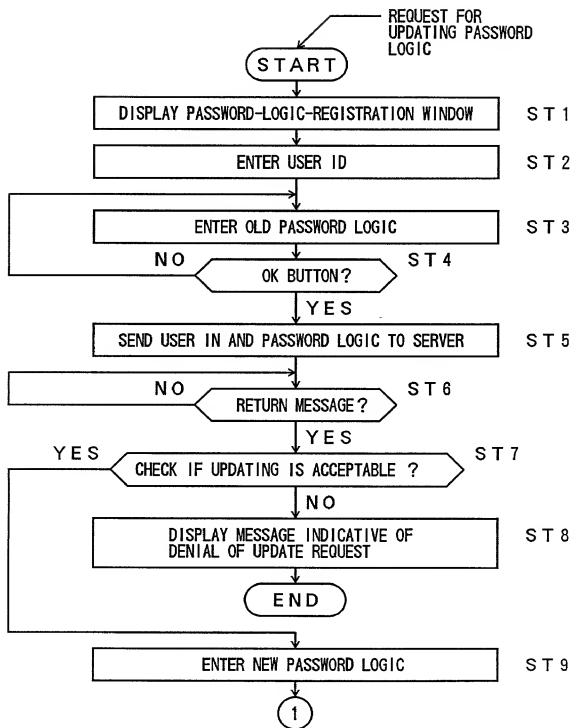


FIG. 13B

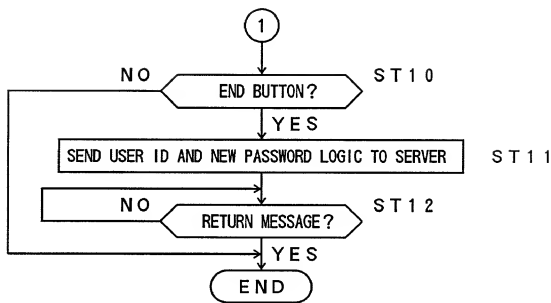


FIG. 14A

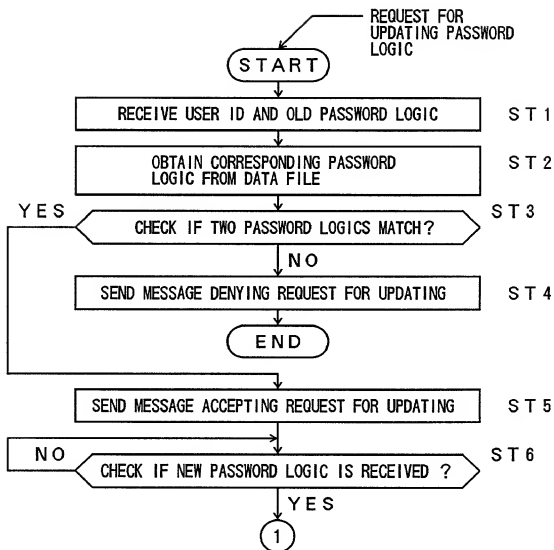


FIG. 14B

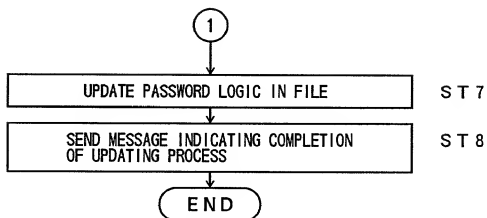


FIG. 15

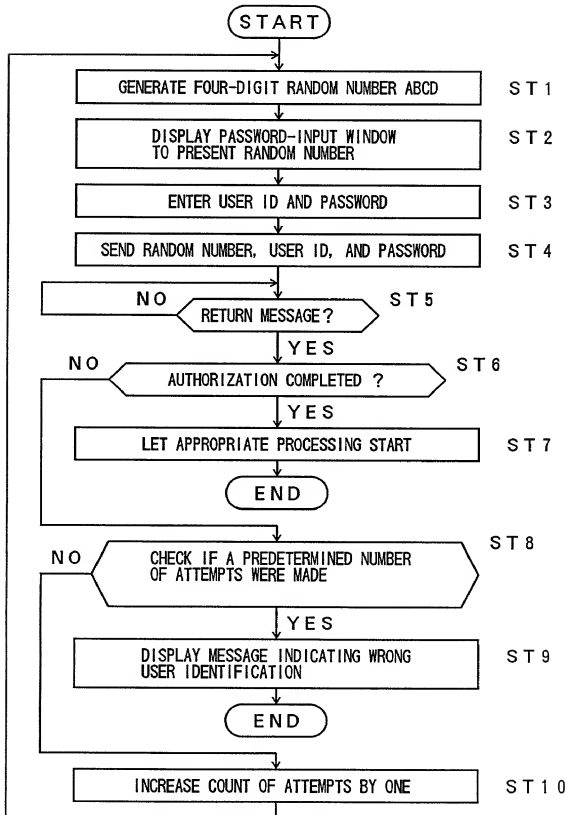


FIG. 16

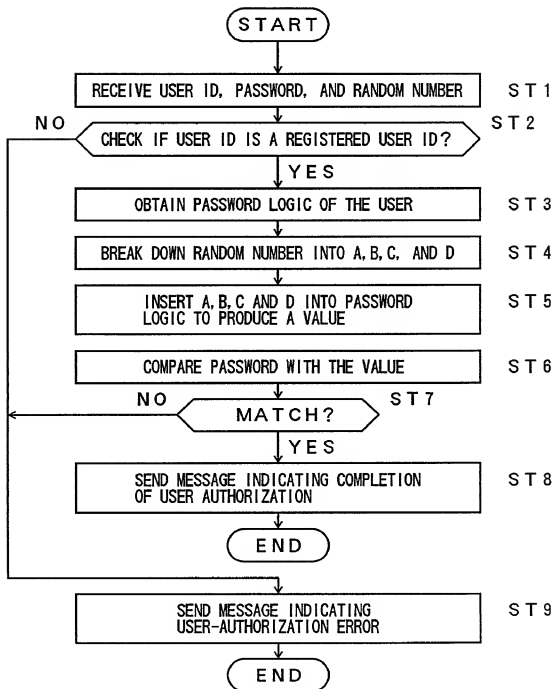


FIG. 17

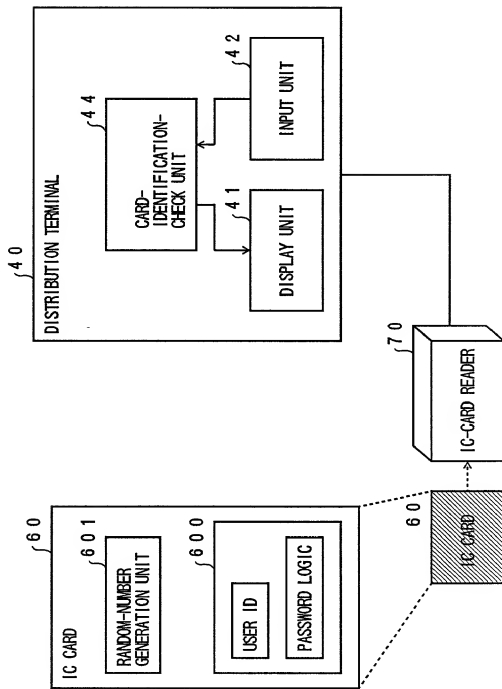


FIG. 18A

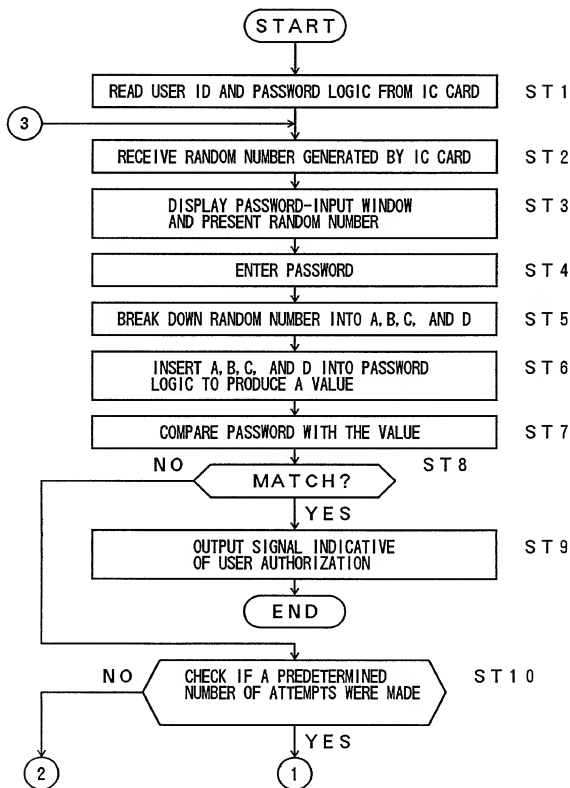
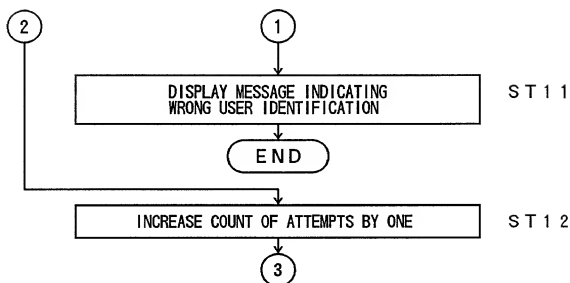


FIG. 18B



Declaration and Power of Attorney For Patent Application

特許出願宣言書及び委任状

Japanese Language Declaration

日本語宣言書

下記の氏名の発明者として、私は以下の通り宣言します。

As a below named inventor, I hereby declare that:

私の住所、私書箱、国籍は下記の私の氏名の後に記載された通りです。

My residence, post office address and citizenship are as stated next to my name.

下記の名称の発明に関して請求範囲に記載され、特許出願している発明内容について、私が最初かつ唯一の発明者（下記の氏名が一つの場合）もしくは最初かつ共同発明者であると（下記の名称が複数の場合）信じています。

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

DEVICE AND METHOD FOR USER IDENTIFICATION

CHECK BASED ON USER-SPECIFIC FORMULA

上記発明の明細書（下記の欄でX印がついていない場合は、本番に添付）は、

the specification of which is attached hereto unless the following box is checked:

☐ 月 日に出発され、米国出願番号または特許協定条約国際出願番号を _____ とし、
（該当する場合） _____ に訂正されました。

☐ was filed on _____
as United States Application Number or
PCT International Application Number
_____ and was amended on
_____ (if applicable).

私は、特許請求範囲をきむ上記訂正後の明細書を検討し、内容を理解していることをここに表明します。

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

私は、通商規則法典第37編第1条56項に定義されるとおり、特許資格の有無について重要な情報を開示する義務があることを認めます。

I acknowledge the duty to disclose information which is material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

Japanese Language Declaration (日本語宣言書)

私は、米国法典第35編119条(a)-(d)項又は365条(b)項に基づき下記の、米国以外の国の少なくとも一か国を指定している特許協力条約365(a)項に基づき国際出願、又は外国での特許出願もしくは発明者証の出願についての外国優先権をここに主張するとともに、優先権を主張している、本出願の前に出願された特許または発明者証の外国出願を以下に、枠内をマークすることで、示しています。

Prior Foreign Application(s)

外国で先行出願
Pat. Appln. No. 11-113058

Japan

21/April/1999

(Number)
(番号)

(Country)
(国名)

(Day/Month/Year Filed)
(出願年月日)

(Number)
(番号)

(Country)
(国名)

(Day/Month/Year Filed)
(出願年月日)

Priority Not Claimed
優先権主張なし

☐

☐

私は、第35編米国法典119条(e)項に基づいて下記の米国特許出願規定に記載された権利をここに主張いたします。

(Application No.)
(出願番号)

(Filing Date)
(出願日)

(Application No.)
(出願番号)

(Filing Date)
(出願日)

私は、下記の米国法典第35編120条に基づいて下記の米国特許出願に記載された権利、又は米国を指定している特許協力条約365条(c)に基づき権利をここに主張します。また、本出願の各請求範囲の内容が米国法典第35編112条第1項又は特許協力条約で規定された方法で先行する米国特許出願に開示されていない限り、その先行米国出願書提出日以降で本出願書の日本国内または特許協力条約国際提出日までの期間中に入手された、連邦規則法典第37編1.56条5項で定義された特許資格の有無に関する重要な情報について開示義務があることを認識しています。

(Application No.)
(出願番号)

(Filing Date)
(出願日)

(Status: Patented, Pending, Abandoned)
(現況: 特許許可済、係属中、放棄済)

(Application No.)
(出願番号)

(Filing Date)
(出願日)

(Status: Patented, Pending, Abandoned)
(現況: 特許許可済、係属中、放棄済)

私は、私自身の知識に基づいて本宣言書中で私が行なう表明が真実であり、かつ私の入手した情報と私の信じていることに基づき表明が全て真実であると信じていること、さらに故意になされた虚偽の表明及びそれと同等の行方は米国法典第18編第1001条に基づき、罰金または有罪、もしくはその両方による処罰されること、そしてそのような虚偽による虚偽の表明を行なえば、出願した、又は英に許可された特許の有効性が失われることを認識し、よってここに上記のごとく宣言を致します。

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Japanese Language Declaration

(日本語宣言書)

委任状: 私は下記の発明者として、本出願に関する一切の手続きを米特許審判局に対して遂行する弁理士または代理人として、下記の者を指名いたします。(弁理士、または代理人の氏名及び登録番号を明記のこと)

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith (list name and registration number)

James D. Halsey, Jr., 22,729; Harry John Staas, 22,010; David M. Pitcher, 25,998; John C. Garvey, 28,607; J. Randall Beckers, 30,358; William F. Herbert, 31,024; Richard A. Gollhofer, 31,106; Mark J. Henry, 36,162; Gene M. Garner II, 34,172; Michael D. Stein, 37,240; Paul I. Kravetz, 35,230; Gerald P. Joyce, III, 37,648; Todd E. Mariette, 35,269; Harlan B. Williams, Jr., 34,756; George N. Stevens, 36,938; Michael C. Soidner, P-41,455 and William M. Schertler, 35,348 (agent)

書類送付先

Send Correspondence to:

STAAS & HALSEY
700 Eleventh Street, N.W.
Suite 500
Washington, D.C. 20001

直接電話連絡先: (名前及び電話番号)

Direct Telephone Calls to: (name and telephone number)

STAAS & HALSEY
(202) 434-1500

唯一または第一発明者名	Full name of sole or first inventor
発明者の署名	Inventor's signature
日付	Date
住所	Residence
国籍	Citizenship
私書箱	Post Office Address
第二共同発明者	Full name of second joint inventor, if any
第二共同発明者	Second inventor's signature
日付	Date
住所	Residence
国籍	Citizenship
私書箱	Post Office Address

Tsuneo Sato
 October 13, 1999
 Kawasaki-shi, Kanagawa, Japan
 Japan
 c/o FUJITSU LIMITED,
 1-1, Kamikodenaka 4-chome, Nakahara-ku,
 Kawasaki-shi, Kanagawa, 211-8588 Japan
 Kiyoshi Koteгава
 October 13, 1999
 Oita-shi, Oita, Japan
 Japan
 c/o FUJITSU OITA SOFTWARE LABORATORIES
 LIMITED, 17-58, Higashikasugamachi.,
 Oita-shi, Oita, 870-8551 Japan

(第三以降の共同発明者についても同様に記載し、署名をすること)

(Supply similar information and signature for third and subsequent joint inventors.)